Atty. Dkt. No. 043034-0164

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kazue SAKO

Title: ANONYMOUS PARTICIPATION AUTHORITY MANAGEMENT SYSTEM

Appl. No.: 09/765,390

Filing Date: 01/22/2001

Examiner: Dada, Beemnet W.

Art Unit: 2135

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service's "Express Mail Post Office To Addressee" service under 37 C.F.R. § 1.10 on the date indicated below and is addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

EV 445623545 US (Express Mail Label Number) July 7, 2005 (Date of Deposit)

Ruthie Vallejo
(Printed Name)

(Signature)

AMENDMENT AND REPLY UNDER 37 CFR 1.116

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This communication is responsive to the Final Office Action dated April 27, 2005, concerning the above-referenced patent application.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this document.

Remarks/Arguments begin on page 10 of this document.

Please amend the application as follows:

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system comprising:

a participant subsystem that is authorized to anonymously participate in a plurality of sessions using secret information provided by a manager subsystem, all of said secret information being transmitted to the participant subsystem prior to participation in a first of said plurality of sessions, said secret information enabling participation in each of the plurality of sessions; and

a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session,

wherein the participant subsystem comprises:

an anonymous signing section for authorizing individual data using the secret information depending on session-related information to produce anonymous participation data with an anonymous signature, and

wherein the reception subsystem comprises:

an anonymous signature determining section for determining whether received data is said anonymous participation data with said anonymous signature authorized by the participant subsystem; and

a sender match determining section for determining whether anonymous signatures of ~~arbitrary~~ two arbitrary pieces of anonymous participation data are signed by an identical participant subsystem.

2. (Original) The system according to claim 1, wherein the anonymous signature includes data that is generated by a predetermined expression using the session-related information and the secret information, wherein the sender match determining section checks the data included in the anonymous signature of received anonymous participation data.

3. (Original) The system according to claim 2, wherein the predetermined expression is represented by raising a session-dependent base to a power that is dependent on the secret information.

4. (Original) The system according to claim 1, wherein the anonymous signing section authorizes the individual data based on a group signature scheme.

5. (Original) The system according to claim 1, wherein the anonymous signing section authorizes the individual data based on an escrowed identity scheme.

6. (Original) The system according to claim 1, wherein the anonymous signing section comprises:

a generator creating section for creating a session-dependent generator depending on the session-related information;

a group signing section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information; and

a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session-related information.

7. (Original) The system according to claim 6, wherein the secret information is represented by (x, y, v) that satisfies: $v = (y + \delta)^{1/e} \bmod n$, where $y = a^x \bmod n$, n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1,

the generator creating section creates a session-dependent generator g_A corresponding to a session A and a generator g_m is generated based on the individual data m and/or the session A,

the group signing section sets $z = g_A^y$ and generates a first proof statement

$V_1 = \mathrm{SKLOGLOG}(z,g_A,a)[\alpha:z = g_A{}^{(a^\alpha)}](1)$

proving the knowledge of α satisfying $z = g_A{}^{(a^\alpha)}$, and a second proof statement

$V_2 = \mathrm{SKROOTLOG}(z*g_A{}^\delta,g_A,e)[\beta: z*g_A{}^\delta = g_A{}^{(\beta^e)}](1)$

proving the knowledge of β satisfying $z*g_A{}^\delta = g_A{}^{(\beta^e)}$,

the linkage data generating section sets $z_1 = g_m{}^y$, and generates a third proof statement

$V_3 = \mathrm{SKREP}(z_1/z, g_m/g_A)[\gamma: z_1/z =(g_m/g_A)^\gamma](1)$

proving the knowledge of z_1 and z have the same power to the bases g_m and g_A, respectively,

wherein the anonymous participation data is defined as $(A, m, z, z_1, V_1, V_2, V_3)$.

8. (Original) The system according to claim 7, wherein

the anonymous signature determining section checks V_1, V_2, and V_3 of the anonymous participation data to determine whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

the sender match determining section checks z of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

9. (Original) The system according to claim 1, wherein the anonymous signing section comprises:

a generator creating section for creating a generator depending on the session-related information;

a group signing section for signing the individual data using the generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information.

10. (Currently Amended) The system according to claim 9, wherein the secret information is represented by (x, y, v) that satisfies: $v = (y + \delta)^{1/e} \bmod n$, where $y = a^x \bmod n$, the individual data is denoted by m, n is a product of two prime numbers as used in the RSA cryptography, g

is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1,

the generator creating section creates a session-dependent generator g_A corresponding to a session A,

the group signing section sets $z = g_A^y$ and generates a first proof statement

$V_1 = \mathrm{SKLOGLOG}(z,g_A,a)[\alpha{:}z = g_A(a^\alpha)](\mathrm{m})$

proving the knowledge of α satisfying $z = g_A(a^\alpha)$, and a second proof statement

$V_2 = \mathrm{SKROOTLOG}(z^*g_A^\delta,g_A,e)[\beta{:}\ z^*g_A^\delta = g_A(\beta^e)](\mathrm{m})$

proving the knowledge of β satisfying $z^*g_A^\delta = g_A(\beta^e)$,

wherein the anonymous participation data~~13~~ is designated as (A, m, z, V_1, V_2).

11. (Original) The system according to claim 10, wherein

the anonymous signature determining section checks V_1, and V_2 of the anonymous participation data to determine whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

the sender match determining section checks z of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

12. (Original) The system according to claim 1, wherein the anonymous signing section comprises:

a generator creating section for creating a session-dependent generator depending on the session-related information;

an escrow identifying section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information; and

a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session-related information.

13. (Original) The system according to claim 12, wherein the secret information is represented by (a, b) that satisfies $b = (a^e - \delta)^{1/e} \bmod n$, where n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1,

the generator creating section creates a session-dependent generator g_A corresponding to a session A and a generator g_m is generated based on the individual data m and/or the session A,

the escrow identifying section sets $z_a = g_A(a^e)$ and generates a first proof statement

$V_1 = \mathrm{SKROOTLOG}(z_a, g_A, e)[\alpha: z_a = g_A(a^e)](1)$

proving the knowledge of α satisfying $z_a = g_A(a^e)$, and sets $z_b = g_A(b^e)$ and generates a second proof statement

$V_2 = \mathrm{SKROOTLOG}(z_b, g_A, e)[\beta: z_b = g_A(b^e)](1)$

proving the knowledge of β satisfying $z_b = g_A(b^e)$, and

the linkage data generating section sets $z_c = g_m(a^e)$ and generates a third proof statement

$V_3 = \mathrm{SKREP}(z_c/z_a, g_m/g_A)[\gamma: z_c/z_a = (g_m/g_A)^\gamma](1)$

proving the knowledge of z_a and z_c having the same power to the bases g_A and g_m, respectively,

wherein the anonymous participation data is defined as $(A, m, z_a, z_b, z_c, V_1, V_2, V_3)$.

14. (Original) The system according to claim 13, wherein

the anonymous signature determining section determines whether $z_a/z_b = g_A{}^\delta$ is satisfied and checks V_1, V_2, and V_3 of the anonymous participation data to determine whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

the sender match determining section checks one of z_a and z_b of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

15. (Original) The system according to claim 1, wherein the anonymous signing section comprises:

a generator creating section for creating a session-dependent generator depending on the session-related information; and

an escrow identifying section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information.

16. (Original) The system according to claim 15, wherein the secret information is represented by (a, b) that satisfies $b = (a^e - \delta)^{1/e} \bmod n$, where n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1,

the generator creating section creates a session-dependent generator g_A corresponding to a session A,

the escrow identifying section sets $z_a = g_A^{(a^e)}$ and generates a first proof statement

$V_1 = \text{SKROOTLOG}(z_a, g_A, e)[\alpha: z_a = g_A^{(a^e)}](\text{m})$

proving the knowledge of α satisfying $z_a = g_A^{(a^e)}$, and sets $z_b = g_A^{(b^e)}$ and generates a second proof statement

$V_2 = \text{SKROOTLOG}(z_b, g_A, e)[\beta: z_b = g_A^{(b^e)}](\text{m})$

proving the knowledge of β satisfying $z_b = g_A^{(b^e)}$,

wherein the anonymous participation data is defined as $(A, m, z_a, z_b, V_1, V_2)$.

17. (Original) The system according to claim 16, wherein

the anonymous signature determining section determines whether $z_a/z_b = g_A^{\delta}$ is satisfied and checks V_1 and V_2 of the anonymous participation data to determine whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and the sender match determining section checks one of z_a and z_b of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

18. (Currently Amended) An anonymous participation authority management method for a system~~, comprising:~~ the system comprising a participant subsystem that is authorized to anonymously participate in a plurality of sessions using secret~~ information;~~ information, and a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session, the method comprising the steps of:

at the participant subsystem,

a) authorizing individual data using the secret information depending on session-related information to produce anonymous participation data with an anonymous signature, all of said secret information being transmitted to the participant subsystem prior to participation in a first of said plurality of sessions, said secret information enabling participation in each of the plurality of sessions;

at the reception subsystem,

b) determining whether received data is said anonymous participation data with said anonymous signature authorized by the participant subsystem; and

c) determining whether anonymous signatures of~~ arbitrary~~ two arbitrary pieces of anonymous participation data are signed by an identical participant subsystem.

19. (Original) The method according to claim 18, wherein the anonymous signature includes data that is generated by a predetermined expression using the session-related information and the secret information, wherein the step (c) is performed by checking the data included in the anonymous signature of received anonymous participation data.

20. (Original) The method according to claim 19, wherein the predetermined expression is represented by raising a session-dependent base to a power that is dependent on the secret information.

21. (Original) The method according to claim 18, wherein the step (a) comprises the steps of:

creating a session-dependent generator depending on the session-related information;

signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information; and

generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session-related information.

22. (Original) The method according to claim 18, wherein the step (a) comprises the steps of:

creating a session-dependent generator depending on the session-related information; and

signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information.

REMARKS

Status of Claims:

Claims 1-22 are present for examination.

Claim Rejections:

Claims 1-6, 9, 12, 15, and 18-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Ateniese et al., "Some Open Issues and New Directions in Group Signatures" (hereinafter Ateniese).

Claims 1-6, 9, 12, 15, and 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ramzan et al., "Group Blind Digital Signatures: A Scalable Solution to Electronic Cash" (hereinafter Ramzan), in view of Ateniese.

Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ateniese in view of Camenisch et al., "Efficient Group Signatures Schemes for Large Groups" (hereinafter Camenisch), and further in view of Grabbe, "Introduction to Digital Cash".

Claims 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ateniese in view of Camenisch.

Claims 13-14 and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ateniese in view of Camenisch, and further in view of Kilian, "Identity Escrow".

With respect to claims 1-22, the rejections are respectfully traversed.

Independent claim 1 recites a system comprising:

> "a participant subsystem that is authorized to anonymously participate in a **plurality** of sessions using secret information provided by a manager subsystem, all of said secret information being transmitted to the participant subsystem prior to participation in a first of said plurality of sessions, said secret information enabling participation in each of the plurality of sessions; and
>
> a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session,

wherein the participant subsystem comprises:

an anonymous signing section for authorizing individual data using the secret information depending on session-related information to produce anonymous participation data with an anonymous signature, and

wherein the reception subsystem comprises:

an anonymous signature determining section for determining whether received data is said anonymous participation data with said anonymous signature authorized by the participant subsystem; and

a sender match determining section for determining whether anonymous signatures of **two arbitrary pieces** of anonymous participation data are signed by an identical participant subsystem." (Emphasis Added).

A system including the above-quoted features has at least the advantages that: (i) a participant subsystem can anonymously participate in a **plurality** of sessions using secret information provided by a manager subsystem where all of the secret information is transmitted to the participant subsystem **prior to participation in a first** of the plurality of sessions and enables participation in each of the sessions; and (ii) a reception subsystem can determine whether anonymous signatures of **two arbitrary pieces** of anonymous participation data are signed by an identical participant subsystem. (Specification; page 22, lines 1-18).

Allowing for a participant subsystem to anonymously participate in a **plurality** of sessions using secret information that is transmitted before a first of the plurality of sessions and that enables participation in each of the plurality of sessions addresses the problem in the prior art systems that employ blind signatures. In the prior art, when blind signatures have been used, a participant subsystem must obtain a signature from a manager subsystem for every session. Thus, when using blind signatures in the prior art, the participant subsystem must **register** with the manager subsystem to obtain a signature from the manager during **every** session. In contrast, a system including the above-quoted features addresses the problem in the prior art by allowing for the same secret information transmitted **prior** to participation in a first session to be used for each of the **plurality** of sessions. Thus, with a system including the above-quoted features, a participant subsystem can participate in a plurality of sessions with only a **single** registration procedure, and it is not necessary to conduct registration processing for every session. (Specification; page 1, line 8 to page 2, line 13; page 5, line 19 to page 7, line 5; page 16, lines 10-13).

Allowing for a reception subsystem to determine whether anonymous signatures of **two arbitrary pieces** of anonymous participation data are signed by an identical participation subsystem addresses the problem in the prior art systems that employ group secret keys. In the prior art, when group secret keys have been employed, use of the group signature makes it impossible to identify the particular participant subsystem in the group to which the group secret key used for generating each signature belonged. Thus, in the prior art systems, if an identical participant subsystem has sent data more than once in a single session, there is no way to verify whether the two signatures have been affixed by using an identical group secret key or not, and therefore, the systems are unable to prevent double voting. Also, the prior art systems are incapable of determining whether two **arbitrary** pieces of anonymous participation data are from an identical participant subsystem, rather than only whether the **same** data has been signed twice by an identical participant subsystem. In contrast, a system including the above-quoted features can determine whether the same participant has participated more than once in the same session even if two **arbitrary** pieces of anonymous participation data from the participant are **different**. (Specification; page 3, line 24 to page 4, line 26; page 5, line 19 to page 7, line 5).

Neither Ateniese nor Ramzan, alone or in combination, disclose or suggest a system including the above-quoted features where: (i) a participant subsystem is authorized to anonymously participate in a **plurality** of sessions using secret information provided by a manager subsystem where all of the secret information is transmitted **prior to participation** in a first of the plurality of sessions and enables participation in each of the plurality of sessions; and (ii) a reception subsystem can determine whether anonymous signatures of two **arbitrary** pieces of anonymous participation data are signed by an identical participant subsystem.

Ateniese examines the use of group signatures for various applications. (Ateniese; abstract). Ateniese begins by reciting the properties of group signatures, and notes that a group signature scheme must satisfy the security property of **unlinkability**, which means that deciding whether two different signatures were computed by the same group member is computationally hard. (Ateniese; section 1, paragraph 1; section 2, paragraph 3, reference "Unlinkability"). Ateniese then later examines the special case of sub-group signatures (SGS). (Ateniese; sections 9-10).

As defined in Ateniese, a SGS is an operation with respect to a **single** message m. (Ateniese; section 9, paragraph 1). The central goal of SGS is to demonstrate that a subset of a certain size of group members has signed a **given** message m. (Ateniese; section 9, paragraph 6). For example, a petition may be circulated among members of a certain group, and a number of members "i" may sign the petition and then publicly announce that "i" members stand behind it, while any insider or outsider is able to verify that "i" distinct members have indeed signed the petition. (Ateniese; section 9, paragraph 5).

Ateniese allows for weakening the unlinkability property **with respect to SGS** in order to achieve compositional integrity in which a verifier can be assured that all signatures comprising a SGS have been generated by distinct signers. (Ateniese; section 9, paragraphs 7 and 8). Thus, a VERIFY procedure for a SGS in Ateniese allows for a verifier to check if a **given** message m has been signed more than once by a given signer. (Ateniese; section 10, paragraph 5).

However, a system as recited in claim 1 including the above-quoted features allows for a reception subsystem to determine whether anonymous signatures of two **arbitrary** pieces of anonymous participation data are signed by an identical participant system. It is important to recognize that the SGS of Ateniese only allows for checking for a redundant signature by a given signer if the message m signed by both signatures is the **same** message m. (Ateniese; section 10). This is because a SGS can be defined only for a **single** message m. This is seen by the "petition" example in Ateniese where only a **single** petition can be signed with one SGS. (Ateniese; section 9, paragraphs 1 and 5).

If two **arbitrary** pieces of anonymous participation data were to be signed with the method of Ateniese, either a regular group signature would be required or two different SGS's would be required. While Ateniese allows for weakening the unlinkability property within a single SGS, Ateniese states that, "we emphasize that this should be done **only** for SGS; i.e., the structure of other types of group signatures (regular, multi-group) must remain unchanged." (Ateniese; section 9, paragraph 8). Thus, in Ateniese, the unlinkability property remains for regular group signatures, so if two **arbitrary** pieces of anonymous participation data were signed with regular group signatures, there would be no way to check if an identical participant subsystem signed both. Also, if two different SGS-s are used for two arbitrarily different messages in the method of Ateniese, it would be computationally difficult to decide whether subgroups that produced the signatures have any member is common. (Ateniese; section 10.1, lemma 2). This is because, in the method of Ateniese, there is a property of unlinkability among different SGS-s. (Ateniese; section 10.1).

Therefore, while Ateniese may allow for determining if a **given** message m has been signed twice by an identical signer, the method of Ateniese does not allow for determining if anonymous signatures of two **arbitrary** pieces of anonymous participation data are signed by an identical participant subsystem, because a SGS in Ateniese is defined only with respect to a **single** message m.

Furthermore, the online voting protocol of Ramzan does not disclose or suggest a system including the above-quoted features, because the online voting protocol of Ramzan requires a registration process for each voting session, and does not allow for a participant subsystem to participate in a **plurality** of sessions using secret information that is transmitted **prior** to participation in a first session and that enables participation in each of the plurality of sessions. Ramzan explicitly states that the online voting scheme proposed, "is similar to the voting scheme based on blind digital signatures." (Ramzan; page 56, section 4.4.4, paragraph 1)(Emphasis Added). As such, during each session of the online voting protocol of Ramzan, there is a **registration** process in which a voter "Alice" must send blinded versions of ballots to a local registration facility (LRF), and the LRF must check a database to make sure that Alice has not voted before and then sign the blinded ballots and give them back to Alice. (Ramzan; page 57, reference "**Online Voting Protocol**", steps 1-3 of "**Registration**").

Therefore, in the online voting scheme of Ramzan, a voter must obtain signatures from a LRF during each session, which requires a **registration step** for each session. This is exactly one of the problems that a system of claim 1 including the above-quoted features was designed to address. (Applicant's specification; page 1, line 8 to page 2, line 13; page 5, line 19 to page 7, line 5). In a system including the above-quoted features, a participant subsystem is authorized to anonymously participate in a **plurality** of sessions using secret information provided by a manager subsystem where all of the secret information is transmitted **prior** to participation in a first of the plurality of sessions and enables participation in each of the plurality of sessions. Thus, with a system including the above-quoted features, there is no need to have a **registration** process for each session.

Moreover, even if the scheme of Ateniese were combined with the scheme of Ramzan, the resulting method would not allow for a participant subsystem to participate in a **plurality** of sessions using secret information that is transmitted **prior** to participation in a first session that enables participation in each of the sessions, and where a reception subsystem can determine whether anonymous signatures of two **arbitrary** pieces of anonymous participation data are signed by an identical participant system. The resulting system would require at least one of the blind digital signatures of Ramzan or the SGS scheme of Ateniese, both of which have deficiencies as recited above.

Therefore, independent claim 1 is neither disclosed nor suggested by the cited prior art and, hence is believed to be allowable. The Patent Office has not made out a *prima facie* case of obviousness under 35 U.S.C. 103.

Independent claim 18 recites an anonymous participation authority management method with features similar to features of a system of independent claim 1. Therefore, independent claim 18 is believed to be allowable for at least the same reasons that claim 1 is believed to be allowable.

The dependent claims are deemed allowable for at least the same reasons indicated above with regard to the independent claims from which they depend.

Conclusion:

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741.

If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date July 7, 2005

By Just Sobaje

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (310) 975-7965
Facsimile: (310) 557-8475

Justin M. Sobaje
Attorney for Applicant
Registration No. 56,252